

PRICE AND GESS

JOSEPH W. PRICE
ALBIN H. GESS
MICHAEL J. MOFFATT
GORDON E. GRAY III
BRADLEY D. BLANCHE

OF COUNSEL
JAMES F. KIRK

ATTORNEYS AT LAW

2100 S.E. MAIN STREET, SUITE 250
IRVINE, CALIFORNIA 92614-6238

A PROFESSIONAL CORPORATION
TELEPHONE: (949) 261-8433
FACSIMILE: (949) 261-9072
FACSIMILE: (949) 261-1726

e-mail: pgu@pgulaw.com

PRIORITY DOCUMENT (Japan 2000-381870)

Jc058 U.S. PTO
10/023021
12/13/01

Inventor(s): Yukiyasu Fukami

Title: BROADCAST APPARATUS AND RECEPTION
APPARATUS FOR PROVIDING A STORAGE SERVICE
BY WHICH SCRAMBLED CONTENT IS STORED AND
DESCRAMBLED USING SCRAMBLING KEY LIST

Attorney's
Docket No.: NAK1-BQ58

EXPRESS MAIL LABEL NO. EL 873069417 US

DATE OF DEPOSIT: December 13, 2001

J W P K I C C 447/261-8750

NIKKEI
Yukiyasu Fukami et al.

10/023021
12/13/01
1c958 U.S. PRO

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application:

2000年12月15日

出願番号

Application Number:

特願2000-381870

出願人

Applicant(s):

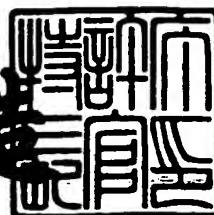
松下電器産業株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 9月13日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造



出証番号 出証特2001-3084745

【書類名】 特許願

【整理番号】 2022520548

【提出日】 平成12年12月15日

【あて先】 特許庁長官殿

【国際特許分類】 H04N 7/16

【発明者】

【住所又は居所】 愛知県名古屋市中区栄2丁目6番1号白川ビル別館5階
株式会社松下電器情報システム名古屋研究所内

【氏名】 深見 幸靖

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式
会社内

【氏名】 中原 徹

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式
会社内

【氏名】 松尾 隆史

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式
会社内

【氏名】 東 吾紀男

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式
会社内

【氏名】 村上 弘規

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100097445

【弁理士】

【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【書類名】 明細書

【発明の名称】 限定受信方法およびシステム

【特許請求の範囲】

【請求項1】 有料番組を配信する放送装置と、前記有料番組を受信して再生する受信装置から構成される限定受信システムであって、

放送装置は、

スクランブル鍵を取得するスクランブル鍵取得手段と、

前記スクランブル鍵からスクランブル鍵リストを作成するスクランブル鍵リスト生成手段と、

前記スクランブル鍵リストを含む蓄積用ECMを作成するECM生成手段と、

前記蓄積用ECMを周期的に送出するECM送出手段と、

前記スクランブル鍵リストからスクランブル鍵を抽出するスクランブル鍵リスト解釈手段と、

抽出した前記スクランブル鍵を用いてコンテンツをスクランブルするスクランブル処理手段と、

前記ECM送出手段から送出された蓄積用ECMと、スクランブルされた前記コンテンツを多重化して有料番組を配信する多重化処理手段を備え、

受信装置は、

受信した有料番組から蓄積用ECMとスクランブルされたスクランブルコンテンツを分離する分離手段と、

分離した前記蓄積用ECMと前記スクランブルコンテンツを蓄積する蓄積手段と、

前記蓄積用ECMからスクランブル鍵リストを抽出するECM解釈手段と、

前記スクランブル鍵リストからスクランブル鍵を抽出するスクランブル鍵リスト解釈手段と、

抽出した前記スクランブル鍵で前記スクランブルコンテンツをデスクランブルするデスクランブル処理手段と、

前記デスクランブルされたコンテンツを再生する再生処理手段を備えたことを特徴とする限定受信システム。

【請求項2】 前記放送装置は、コンテンツをTSパケット化するTSパケット化処理手段と、

前記TSパケットをひとつずつ取得し、取得したTSパケットが先頭から何番目かをカウントするTSパケットカウンタ手段をさらに備え、

前記スクランブル鍵リスト解釈手段は、前記TSパケットのカウント値を基に前記スクランブル鍵リストからスクランブル鍵を抽出し、

一方、前記受信装置は、前記蓄積手段に蓄積されている前記スクランブルコンテンツからひとつずつTSパケットを取り出し、取り出したTSパケットが先頭から何番目かをTSパケットインデックスとしてカウントするTSパケット抽出手段をさらに備え、

前記スクランブル鍵リスト解釈手段は、前記TSパケットのTSパケットインデックス値を基に前記スクランブル鍵リストからスクランブル鍵を抽出することを特徴とする請求項1に記載の限定受信システム。

【請求項3】 前記放送装置の前記ECM生成手段は、前記スクランブル鍵リストをECMのデータ形式のうち、暗号化対象部分に埋め込んで蓄積用ECMを作成することを特徴とする請求項1に記載の限定受信システム。

【請求項4】 前記放送装置の前記ECM生成手段は、従来のECMと蓄積用ECMを区別する情報を埋め込んだ形式で蓄積用ECMを作成することを特徴とする請求項1に記載の限定受信システム。

【請求項5】 前記ECM送出手段は、前記蓄積用ECMを1回だけ送出することを特徴とする請求項1に記載の限定受信システム。

【請求項6】 前記放送装置は、コンテンツをTSパケット化するTSパケット化処理手段と、

前記TSパケットの非スクランブルな特定の情報を取り出して解釈するTSパケットヘッダ解釈手段をさらに備え、

前記スクランブル鍵リスト解釈手段は、前記特定の情報を基に前記スクランブル鍵リストからスクランブル鍵を抽出し、

一方、前記受信装置は、前記蓄積手段に蓄積されている前記スクランブルコンテンツからひとつずつTSパケットを取り出し、前記TSパケットの非スクラン

ブルな特定の情報を取り出すT Sパケット抽出手段をさらに備え、

前記スクランブル鍵リスト解釈手段は、前記特定の情報を基に前記スクランブル鍵リストからスクランブル鍵を抽出する

ことを特徴とする請求項1に記載の限定受信システム。

【請求項7】 前記放送装置は、前記特定の情報に対して演算を行うスクランブル鍵識別子算出手段をさらに備え、

前記スクランブル鍵リスト解釈手段は、演算された前記特定の情報を基に前記スクランブル鍵リストからスクランブル鍵を抽出し、

一方、前記受信装置は、前記特定の情報に対して演算を行うスクランブル鍵識別子算出手段をさらに備え、

前記スクランブル鍵リスト解釈手段は、演算された前記特定の情報を基に前記スクランブル鍵リストからスクランブル鍵を抽出する
ことを特徴とする請求項6に記載の限定受信システム。

【請求項8】 受信した有料番組から蓄積用ECMとスクランブルされたスクランブルコンテンツを分離する分離手段と、

分離した前記蓄積用ECMと前記スクランブルコンテンツを蓄積する蓄積手段と、

前記蓄積用ECMからスクランブル鍵リストを抽出するECM解釈手段と、

前記蓄積手段に蓄積されている前記スクランブルコンテンツからひとつずつT Sパケットを取り出し、取り出したT Sパケットが先頭から何番目かをT SパケットインデックスとしてカウントするT Sパケット抽出手段と、

前記T SパケットのT Sパケットインデックス値を基に前記スクランブル鍵リストからスクランブル鍵を抽出するスクランブル鍵リスト解釈手段と、

抽出した前記スクランブル鍵で前記スクランブルコンテンツをデスクランブルするデスクランブル処理手段と、

前記デスクランブルされたコンテンツを再生する再生処理手段
を備えたことを特徴とする受信装置。

【請求項9】 前記T Sパケット抽出手段は、ひとつのT Sパケットを抽出する毎に、当該パケットがIピクチャであるか判断し、Iピクチャである場合にの

み前記T Sパケットを前記デスクランブル処理手段へ送ることで特殊再生を行うことを特徴とする請求項8に記載の受信装置。

【請求項10】 前記E CM解釈手段で抽出したスクランブル鍵リストを保持するスクランブル鍵リスト保持手段と、前記スクランブル鍵リスト解釈手段をセキュリティモジュール内部に備えることを特徴とする請求項8に記載の受信装置。

【請求項11】 有料番組を配信する放送装置と、前記有料番組を受信して再生する受信装置から構成される限定受信方法であって、

放送装置は、

スクランブル鍵を取得するスクランブル鍵取得ステップと、

前記スクランブル鍵からスクランブル鍵リストを作成するスクランブル鍵リスト生成ステップと、

前記スクランブル鍵リストを含む蓄積用E CMを作成するE CM生成ステップと、

前記蓄積用E CMを周期的に送出するE CM送出ステップと、

前記スクランブル鍵リストからスクランブル鍵を抽出するスクランブル鍵リスト解釈ステップと、

抽出した前記スクランブル鍵を用いてコンテンツをスクランブルするスクランブル処理ステップと、

前記E CM送出手段から送出された蓄積用E CMと、スクランブルされた前記コンテンツを多重化して有料番組を配信する多重化処理ステップを備え、

受信装置は、

受信した有料番組から蓄積用E CMとスクランブルされたスクランブルコンテンツを分離する分離ステップと、

分離した前記蓄積用E CMと前記スクランブルコンテンツを蓄積する蓄積ステップと、

前記蓄積用E CMからスクランブル鍵リストを抽出するE CM解釈ステップと

前記スクランブル鍵リストからスクランブル鍵を抽出するスクランブル鍵リスト解釈ステップと、

抽出した前記スクランブル鍵で前記スクランブルコンテンツをデスクランブルするデスクランブル処理ステップと、

前記デスクランブルされたコンテンツを再生する再生処理ステップを備えたことを特徴とする限定受信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、デジタル放送における限定受信方法およびシステムに関し、特に、蓄積型サービスにおける有料番組のスクランブル鍵送出方法に関する。

【0002】

【従来の技術】

現在のBSデジタル放送のCA (C o n d i t i o n a l A c c e s s) 方式では、ECMに現在と次のスクランブル鍵を記述して送出される。また、チャネル切替時に、映像および音声が出力されるまでの時間を短縮するなどの改良をした発明（特開平11-340966）がある。

【0003】

【発明が解決しようとする課題】

しかしながら、コンテンツをHDDなどに蓄積した後で、コンテンツを視聴または購入する蓄積型サービスの開始が予定されている。その際にスクランブルコンテンツを蓄積後に特殊再生（早送り再生、巻き戻し再生など）やランダムアクセス（コンテンツの任意の場所から再生）を行う場合、従来の方式によると、視聴対象となる部分に対応するスクランブル鍵すなわちECM（Entitlement Control Message：共通情報）を、蓄積したTS（Transport Stream）の中から検出し、スクランブル鍵を抽出した後でデスクランブル処理を行う必要がある。そのために、例えば早送り再生機能の性能が、十分ユーザの満足できるスピードにならない可能性がある。

【0004】

本発明は、スクランブルコンテンツを蓄積し、蓄積後の特殊再生機能を、ユーザーの満足できる性能で実現することを目的とする。

【0005】

【課題を解決するための手段】

この課題を解決するために本発明は、有料番組を配信する放送装置と、前記有料番組を受信して再生する受信装置から構成される限定受信システムであって、放送装置は、スクランブル鍵を取得するスクランブル鍵取得手段と、前記スクランブル鍵からスクランブル鍵リストを作成するスクランブル鍵リスト生成手段と、前記スクランブル鍵リストを含む蓄積用ECMを作成するECM生成手段と、前記蓄積用ECMを周期的に送出するECM送出手段と、前記スクランブル鍵リストからスクランブル鍵を抽出するスクランブル鍵リスト解釈手段と、抽出した前記スクランブル鍵を用いてコンテンツをスクランブルするスクランブル処理手段と、前記ECM送出手段から送出された蓄積用ECMと、スクランブルされた前記コンテンツを多重化して有料番組を配信する多重化処理手段を備え、一方、受信装置は、受信した有料番組から蓄積用ECMとスクランブルされたスクランブルコンテンツを分離する分離手段と、分離した前記蓄積用ECMと前記スクランブルコンテンツを蓄積する蓄積手段と、前記蓄積用ECMからスクランブル鍵リストを抽出するECM解釈手段と、前記スクランブル鍵リストからスクランブル鍵を抽出するスクランブル鍵リスト解釈手段と、抽出した前記スクランブル鍵で前記スクランブルコンテンツをデスクランブルするデスクランブル処理手段と、前記デスクランブルされたコンテンツを再生する再生処理手段を備えたことを特徴とする。

【0006】

【発明の実施の形態】

以下、本発明の実施の形態について図面を用いて説明する。

【0007】

(実施の形態1)

図1は、本発明の実施の形態1によるシステム全体の構成を示す図である。システムは放送装置100と、受信機200とセキュリティモジュール300から

構成されている。なお、セキュリティモジュール300は、物理的には通常ICカードとして実現され、受信機200にセットして使用される。放送装置100は、TSパケット化処理部101と、スクランブル鍵リスト生成部102と、スクランブル処理部103と、ECM生成部104と、ECM送出部105と、多重化処理部106と、コンテンツ取得部107と、スクランブル鍵取得部108とから構成されている。受信機200は、TS分離部201と、蓄積装置であるHDD202と、スクランブル鍵リスト保持部203と、デスクランブル処理部204と、再生処理部205とから構成されている。セキュリティモジュール300は、ECM解釈部301から構成されている。

【0008】

図2は放送装置100のスクランブル処理部103の構成をさらに詳しく示した図である。スクランブル処理部103は、TSパケットカウンタ部110と、スクランブル鍵リスト保持部111と、スクランブル部112と、スクランブル鍵リスト解釈部113からなる。

【0009】

なお、図1、図2では現行BSデジタル放送システムとの違いを明記するために、蓄積用ECMを作成して送出する系とは異なる現行BSデジタル放送システムにおけるECMを作成して送出する系も併記しており、スクランブル鍵取得部108で取得したスクランブル鍵をスクランブル処理部103およびECM生成部104へ渡す部分が現行BSデジタル放送システムでの系である（図中点線で示している）。

【0010】

図3は受信機200のデスクランブル処理部204の構成をさらに詳しく示した図である。デスクランブル処理部204は、TSパケット抽出部210と、デスクランブル部211と、スクランブル鍵リスト解釈部212からなる。

【0011】

次にTSパケットとスクランブルキーの対応（スクランブル鍵リストから該当TSパケットのスクランブル鍵を抽出するための情報）をECM（Entitlement Control Message：共通情報）に記述する方法につ

いて放送装置側における詳細な動作および、受信機側における詳細な動作について説明する。

【0012】

(放送装置側)

図4は放送装置100において映像、音声、データなどのコンテンツにスクランブルをかける際の動作手順を示すフローチャートである。図1と図2も用いて説明する。まず、スクランブル鍵取得部108でスクランブル鍵を取得し、取得したスクランブル鍵をスクランブル鍵リスト生成部102へ渡す(ステップS501)。次に、スクランブル鍵リスト生成部102でスクランブル鍵リストを作成する(ステップS502)。スクランブル鍵リストの一例としては、図9にデータ構造を示すようなスクランブル鍵リスト記述子がある。スクランブル鍵リスト記述子は、スクランブル鍵の識別をするスクランブル鍵識別子(Ks_id)とスクランブル鍵(Ks)と当該KsでスクランブルするTSパケット数(TS_packet_number)から構成され、Ksの数分Ks_idとKsとTS_packet_numberとが記述される。次に、ECM生成部104において、図8にデータ構造を示すように、BSデジタル放送方式で規定されているECM本体の可変部(暗号化対象)に、上記スクランブル鍵リスト記述子を追加することによって、蓄積用ECMを作成し(ステップS503)、ECM送出部105から多重化処理部106へ送出する(ステップS504)。蓄積用ECMとは蓄積再生機能(蓄積したコンテンツをタイムシフト視聴できる機能)用に使用するECMであり、従来のECMと区別するための情報を埋め込む。上記ステップS503で、例えば、図8に示すように、セクションヘッダ部のテーブル識別子の値を、従来のECMと蓄積用ECMで異なる値にする。なお、テーブル識別子は同じ値にして、拡張テーブル識別子の値を異なる値にしてもよい。一方、コンテンツ取得部107で取得した映像、音声、データなどのコンテンツを、TSパケット化処理部101においてTSパケット化し(ステップS505)、スクランブル処理部103でスクランブルをかけ(ステップS506)、多重化処理部106においてスクランブルコンテンツと蓄積用ECMを多重化した(ステップS507)有料番組をTSとして放送する。本明細書ではスクランブル

コンテンツと蓄積用ECMを多重化したものを有料番組と定義する。

【0013】

なお、図1はスクランブル鍵、コンテンツを放送装置100とは別の装置で作成する前提で記述したが、スクランブル鍵、コンテンツとともに放送装置100内で作成してもよいし、どちらか一方のみ放送装置100内で作成してもかまわない。

【0014】

次に、図5にスクランブル処理部103の処理（図4ステップS506）の詳細フローチャートを示す。スクランブル鍵リスト生成部102から、スクランブル鍵リストを取得し、スクランブル鍵リスト保持部111に格納する（ステップS601）。TSパケット化処理部101にTSパケット化された（ステップS504）コンテンツをTSパケットカウンタ部110において、1TSパケット分取得する（ステップS602）。1TSパケット分取得した時にTSパケットカウンタ部110は、TSパケット数を累積することによって、当該TSパケットが先頭から何番目のパケットかをカウントし、TSパケット累積数（先頭から何番目のパケットかの情報）をスクランブル鍵リスト解釈部113へ渡し、TSパケットをスクランブル部112へ渡す（ステップS603）。なお、TSパケット累積数は、別のコンテンツに対して図4のフローチャートに示す処理をする前にリセットしておく。次に、スクランブル鍵リスト解釈部113において、TSパケット累積数とスクランブル鍵リスト保持部111に格納してあるスクランブル鍵リストから該当スクランブル鍵を抽出して、スクランブル部112へ渡す（ステップS604）。スクランブル部112において、ステップS603で取得した1TSパケット分を、ステップS604で取得したスクランブル鍵でスクランブルをかけ、多重化処理部106へ渡し（ステップS605）、全TSパケット分取得したかどうかを判定して（ステップS606）、取得完了していれば処理を終了し、そうでなければ、ステップS602からの処理を繰り返す。

【0015】

以下に図10に示すような、説明のため簡略した具体例を用いて、ステップS604の詳細な説明を行う。図10の例ではスクランブルをかけたいコンテンツ

TSが400TSパケットから構成され、先頭から100パケット分単位で、スクランブル鍵を変更する例である。図10の例におけるスクランブル鍵リストの具体例を図11に示す。

【0016】

図10において2番目のパケットであるTSP2をスクランブルする際に、該当スクランブル鍵を抽出する時の処理を示す。2番目のTSパケットなのでTSパケット累積数は2であり、図11のスクランブル鍵リストによると、先頭から100番目までのTSパケットのスクランブル鍵はKs1であるため、TSP2の該当スクランブル鍵はKs1であり、Ks1を抽出する。同様にTSP100までの該当スクランブル鍵はKs1である。TSP101になると、TSパケット累積数は101番目のTSパケットなので101であり、図11のスクランブル鍵リストによると、スクランブル鍵はKs1ではなく次のKs2である。

【0017】

(スクランブル鍵リスト送出タイミング)

次に、スクランブル鍵リストの送出タイミングの説明をする。スクランブル鍵リストはスクランブルコンテンツに対して少なくとも一つ、蓄積すれば良いため図19に示すように、現行BSデジタル方式における送出周期に比べて、長い周期(例えば10倍程度)で送出すればよい。また確実に蓄積される保証があれば、スクランブルコンテンツに対して1度だけ送出してもよい。

【0018】

(受信機側)

図6はTS分離部201で、テーブル識別子または拡張テーブル識別子の値によって、従来のECMと区別することによって蓄積用ECMとスクランブルコンテンツを分離してHDD202に蓄積後に、受信機200でスクランブルコンテンツをデスクランブルする際の動作手順を示すフローチャートである。図1と図3も用いて説明する。なお、蓄積用ECMとスクランブルコンテンツを分離せずに、一時的に一つのTSとして蓄積し、蓄積後に分離してもよい。

【0019】

まず、HDD202に蓄積してある蓄積用ECMをセキュリティモジュール3

00内のECM解釈部301へ渡す（ステップS701）。ECM解釈部301で蓄積用ECMからスクランブル鍵リストを抽出する（ステップS702）。ECM解釈部301から取得したスクランブル鍵リストをスクランブル鍵リスト保持部203に格納する（ステップS703）。一方、HDD202に蓄積してあるスクランブルコンテンツをデスクランブル処理部204へ渡し（ステップS704）、デスクランブル処理部204でデスクランブルする（ステップS705）。

【0020】

図7にデスクランブル処理部204の処理（ステップS705）の詳細フローチャートを示す。ステップS704で渡されたスクランブルコンテンツをTSパケット抽出部210において、1TSパケット分抽出する（ステップS801）。1TSパケット分抽出した時にTSパケット抽出部210は、当該TSパケットが先頭から何番目のパケットかをカウントし、その情報（以下、TSパケットインデックスと記述）を、スクランブル鍵リスト解釈部212へ渡し、抽出したTSパケットをデスクランブル部211へ渡す（ステップS802）。スクランブル鍵リスト解釈部212において、TSパケットインデックスとスクランブル鍵リスト保持部203に格納してあるスクランブル鍵リストから該当スクランブル鍵を抽出して、デスクランブル部211へ渡す（ステップS803）。デスクランブル部211において、ステップS802で取得した1TSパケット分を、ステップS803で取得したスクランブル鍵でデスクランブルし、再生処理部へ渡す（ステップS804）。全TSパケット分取得したかどうかを判定して（ステップS805）、取得完了していれば処理を終了し、そうでなければ、ステップS801からの処理を繰り返す。

【0021】

（特殊再生する際の受信機の詳細な動作）

次に、蓄積後のスクランブルコンテンツを特殊再生する際の受信機の詳細な動作について説明する。ここでは、特殊再生の代表的機能である早送り再生機能について説明する。MPEG2符号化方式では、映像ストリームは図21に示すようにIピクチャ（フレーム内符号化画像）、Bピクチャ（双方向予測符号化画像

)、Pピクチャ(フレーム間順方向予測符号化画像)の三種類のピクチャから構成され、Iピクチャのみ単独で復号することが可能なため、早送り再生機能は、ピクチャのみを再生することで実現する。次に、図21で示す映像ストリームをTSに変換した模式図を図12に示す。図12では簡易的に、図21のIピクチャを、図12の斜線部分のTSパケットに変換したと仮定する。すなわち最初のIピクチャがTSP2～TSP5へ、二番目のIピクチャがTSP101からTSP104へ、三番目のIピクチャがTSP201～TSP204へ、四番目のIピクチャがTSP301～TSP304へ変換できたとする。

【0022】

以下、斜線部分のTSパケットをデスクランブルする際の受信機の動作手順を説明する。スクランブル鍵リストは図11に示す。フローチャートは前述の図6には変更がなく、デスクランブル処理部の処理に一部変更があるため、デスクランブル処理部の処理を図22に示し、図7も用いて説明する。まず、TSパケット抽出部210において、スクランブルコンテンツを1TSパケット分抽出し(ステップS1101)、特殊再生処理かどうか判定して(ステップS1102)、特殊再生処理であればステップS1103へ移り、特殊再生処理でなければステップS1104へ移る。次に、TSパケット抽出部210において抽出したパケットがIピクチャかどうか判定して(ステップS1103)、IピクチャであればステップS1104へ移り、Iピクチャでなければ、ステップS1101へ戻る。ステップS1104以降の処理は、図7のステップS802以降と同様なので、図12に示す具体例で説明する。例えばIピクチャであるTSP2を抽出した時は、二番目のパケットなのでステップS1104でTSパケットインデックスを2と算出する。次に、ステップS1105で、図11のスクランブル鍵リストから該当スクランブル鍵Ks1を抽出し、ステップS1106で、TSP2をスクランブル鍵Ks1でデスクランブルする。同様に、TSP3～TSP5をスクランブル鍵Ks1でデスクランブルし、TSP101～TSP104をスクランブル鍵Ks2で、TSP201～TSP204をスクランブル鍵Ks3で、TSP301～TSP304をスクランブル鍵Ks4でデスクランブルする。

【0023】

ステップS1103におけるIピクチャかどうかを判定する方法は、例えば特開平8-340541に記述があるように、TSパケットの非スクランブル部分にIピクチャであることがわかるような情報を送出時に埋め込んでおき、その情報を見て判定する。

【0024】

なお、巻き戻し再生機能は、TSパケットの抽出順序を早送り再生機能の時と逆にすることで実現可能である。また、ランダムアクセス機能は、抽出するTSパケットの開始位置が異なるだけで、それ以外は同様な処理で実現可能である。つまり、デスクランブル対象である任意のTSパケットに対するスクランブル鍵を、スクランブル鍵リストから抽出することによって種々の特殊再生等が実現できる。

【0025】

(実施の形態2)

実施の形態1では、受信機内のセキュリティが保証されることを前提として、スクランブル鍵リスト保持部203およびスクランブル鍵リスト解釈部212が受信機内にある構成で説明した。しかし、図13に示すように、スクランブル鍵リスト保持部203およびスクランブル鍵リスト解釈部212がセキュリティモジュール300内にある構成にすれば、スクランブル鍵リストの安全性を高めることができる。図14にデスクランブル処理部の詳細図を示す。

【0026】

フローチャートは実施の形態1で説明した図6、図7と同様であるが（ただし図6のデスクランブル処理部での処理（S705）はデスクランブル処理部とセキュリティモジュールでの処理になる）、図7のステップS803はセキュリティモジュール内での処理になる。また、ステップS803において、スクランブル鍵をセキュリティモジュール300からデスクランブル部へ渡す時には暗号をかけ、受信機での処理が終了後はすぐに受信機内のメモリ上からスクランブル鍵を削除すればよい。

【0027】

(実施の形態3)

次に、TSパケットとスクランブルキーの対応をECMへの記述と、TSパケットの非スクランブル部とを利用する方法について説明する。ここでの方法によれば、図9のデータ構造中TS_packet_numberが不要になるため、伝送容量の節約にもなる。

【0028】

以下、TSパケットの非スクランブル部の中のCC (Continuity Counter) を利用する方法について説明する。CCとはTSパケットヘッダーの4ビットを使用した巡回カウンタ（値0から1ずつ増加して15までいたら0に戻る）で、同じパケットIDを持つTSパケットが途中で一部破棄されたかどうかを検出するための情報であり、国際標準規格MPEG2システムで規定されている。

【0029】

本発明の実施の形態3によるシステム全体の構成は、実施の形態1による構成である図1と同様であるが、その中のスクランブル処理部103とデスクランブル処理部204の構成が異なるので、図15にスクランブル処理部103の構成を図16にデスクランブル処理部の構成を示す。

【0030】

スクランブル処理部103は、スクランブル鍵識別子算出部120と、TSパケットヘッダ解釈部121と、スクランブル鍵リスト保持部122と、スクランブル部123と、スクランブル鍵リスト解釈部124からなる。

【0031】

デスクランブル処理部204は、TSパケット抽出部220と、スクランブル鍵識別子算出部221と、デスクランブル部222と、スクランブル鍵リスト解釈部223からなる。

【0032】

（放送装置側）

放送装置100において映像、音声、データなどのコンテンツにスクランブルをかける際の動作手順を示すフローチャートは図4と同様であるが、スクランブル処理部103における処理（ステップS505）が異なるので、図17にその

フローチャートを示す。図1と図15も用いて説明する。

【0033】

スクランブル鍵リスト生成部102から、スクランブル鍵リストを取得し、スクランブル鍵リスト保持部122に格納する（ステップS901）。TSパケット化処理部101でTSパケット化された（ステップS504）コンテンツをTSパケットヘッダ解釈部121において、1TSパケット分取得する（ステップS902）。1TSパケット分取得した時にTSパケットヘッダ解釈部121は、CCの値を読み取り、読み取ったCCの値をスクランブル鍵識別子算出部120へ渡し、TSパケットをスクランブル部123へ渡す（ステップS903）。スクランブル鍵識別子算出部120において、CCの値からスクランブル鍵識別子を算出し、スクランブル鍵リスト解釈部124へ渡す（ステップS904）。スクランブル鍵リスト解釈部124においてスクランブル鍵識別子とスクランブル鍵リスト保持部122に格納してあるスクランブル鍵リストから該当スクランブル鍵を抽出して、スクランブル部123へ渡す（ステップS905）。スクランブル部123において、ステップS903で取得した1TSパケット分を、ステップS905で取得したスクランブル鍵でスクランブルをかけ、多重化処理部106へ渡し（ステップS906）、全TSパケット分取得したかどうかを判定して（ステップS907）、取得完了していれば処理を終了し、そうでなければ、ステップS902からの処理を繰り返す。ステップS904におけるCCの値からスクランブル鍵識別子を算出する方法には、例えば、 $CC \bmod n$ ($1 \leq n \leq 16$)（なお、 \bmod とは、CCをnで割った余りである）の値をスクランブル鍵識別子とする方法がある。この算出方法によれば、CCの値は0から15までの値をとるために、 $n = 16$ の場合、スクランブル鍵リストは図20に示すように、識別子0から15までの16個のスクランブル鍵から構成される。例えばCCの値が2のTSパケットは、2を16で割った余りが2なので識別子の値は2となり、スクランブル鍵Ks3を使ってスクランブルする。なお、スクランブル鍵をCCの値から算出する方法にすることにより、CCの値をそのままスクランブル鍵識別子とするより、スクランブル鍵識別子の値が見破られることを防止できる。

【0034】

n の値を16として説明したが、1から15までの値でもかまわない。 n の値を変更することによって、スクランブル鍵リストを作成した後で、再度作成し直すことなく使用するスクランブル鍵の数を容易に変更できる。例えば、図20に示すようなスクランブル鍵リストを変更せずに、 n の値を4に変更することにより、識別子の値は0から3までとなり、使用するスクランブル鍵はKs1、Ks2、Ks3、Ks4の4つとなる。なお、 n の値は算出方法として、予め固定値としてもよいし、図8に示した蓄積用ECMの可変部に記述してもよい。

【0035】

また、CCの値を利用するのではなく、CCと同様に国際標準規格MPEG2システムで規定されているプログラム時刻基準参照値であるPCR (Program Clock Reference)、またはオリジナルプログラム時刻基準参照値であるOPCR (Original PCR) の特定のビット（例えば、4ビットにすればCCと全く同様に処理することができる）を利用してかまわない。

【0036】

また、既に使用方法がMPEG2システムで規定されている領域を利用するのではなく、アダプテーション・フィールド部のプライベートデータ領域のようにユーザが自由に使用できる領域に、スクランブル鍵識別子の値を直接記述してもよい。

【0037】

（受信機側）

TS分離部201で蓄積用ECMとスクランブルコンテンツを分離してHDD202に蓄積後に、受信機200でスクランブルコンテンツをデスクランブルする際の動作手順を示すフローチャートは図6と同様であるが、デスクランブル処理部204における処理（ステップS705）が異なるので、図18にそのフローチャートを示す。図1と図16も用いて説明する。なお、蓄積用ECMとスクランブルコンテンツを分離せずに一つのTSとして蓄積してもよい。

【0038】

ステップS704で渡されたスクランブルコンテンツをTSパケット抽出部220において、1TSパケット分抽出する（ステップS1001）。1TSパケット分抽出した時にTSパケット抽出部220は、当該TSパケットのCCの値を読み取り、読み取ったCCの値を、スクランブル鍵識別子算出部221へ渡し、抽出したTSパケットをデスクランブル部222へ渡す（ステップS1002）。スクランブル鍵識別子算出部221において、CCの値からスクランブル鍵識別子を算出し、スクランブル鍵リスト解釈部223へ渡す（ステップS1003）。スクランブル鍵リスト解釈部223においてスクランブル鍵識別子とスクランブル鍵リスト保持部203に格納してあるスクランブル鍵リストから該当スクランブル鍵を抽出して、デスクランブル部222へ渡す（ステップS1004）。デスクランブル部222において、ステップS1002で取得した1TSパケット分を、ステップS1004で取得したスクランブル鍵でデスクランブルし、再生処理部へ渡す（ステップS1005）。全TSパケット分取得したかどうかを判定して（ステップS1006）、取得完了していれば処理を終了し、そうでなければ、ステップS1001からの処理を繰り返す。

【0039】

ステップS1003におけるCCの値からスクランブル鍵識別子を算出する方法は、前述の放送装置で説明した方法と同じである。

【0040】

【発明の効果】

本発明では、スクランブル鍵リストを送出することによって、蓄積後のスクランブルコンテンツを再生する場合に、再生対象となる任意のTSパケットに対応するスクランブル鍵を、スクランブル鍵リストから即座に抽出することができる。

【0041】

スクランブル鍵リストの送出周期は長周期にすることができるので、伝送容量の節約ならびに、送出装置の送出タイミング制御処理を軽減することが容易である。

【0042】

また、一つのコンテンツに対して複数のスクランブル鍵を使用することによって従来通りのセキュリティ強度も保証できる。

【0043】

さらに、スクランブル鍵リストをセキュリティモジュール内に格納することにより、スクランブル鍵リストが悪質なユーザによって見破られることを防止することができる。

【0044】

以上のように、スクランブルコンテンツを蓄積し、蓄積後の特殊再生機能を、ユーザの満足できる性能で、またセキュリティ強度も保証した方法で実現できる。

【図面の簡単な説明】

【図1】

システムの全体構成図

【図2】

本発明の実施の形態1におけるスクランブル処理部の構成図

【図3】

本発明の実施の形態1におけるデスクランブル処理部の構成図

【図4】

本発明の実施の形態1における放送装置の動作手順を示すフローチャート

【図5】

本発明の実施の形態1におけるスクランブル処理部の動作手順を示すフローチャート

【図6】

本発明の実施の形態1における受信機の動作手順を示すフローチャート

【図7】

本発明の実施の形態1におけるデスクランブル処理部の動作手順を示すフローチャート

【図8】

蓄積用ECMのデータ構造の例を示す図

【図9】

スクランブル鍵リスト記述子のデータ構造の例を示す図

【図10】

フローチャートの補足説明する具体例を示す図

【図11】

スクランブル鍵リストの具体例を示す第一の図

【図12】

早送り再生機能を説明するための具体例を示す図

【図13】

本発明の実施の形態2における受信機の構成図

【図14】

本発明の実施の形態2におけるデスクランブル処理部の構成図

【図15】

本発明の実施の形態3におけるスクランブル処理部の構成図

【図16】

本発明の実施の形態3におけるデスクランブル処理部の構成図

【図17】

本発明の実施の形態3におけるスクランブル処理部の動作手順を示すフローチャート

【図18】

本発明の実施の形態3におけるデスクランブル処理部の動作手順を示すフローチャート

【図19】

スクランブル鍵リストの送出タイミングを示す図

【図20】

スクランブル鍵リストの具体例を示す第2の図

【図21】

MPEG2符号化方式による映像ストリームの概念図

【図22】

本発明の実施の形態1における早送り再生時のデスクランブル処理部の動作手順を示すフローチャート

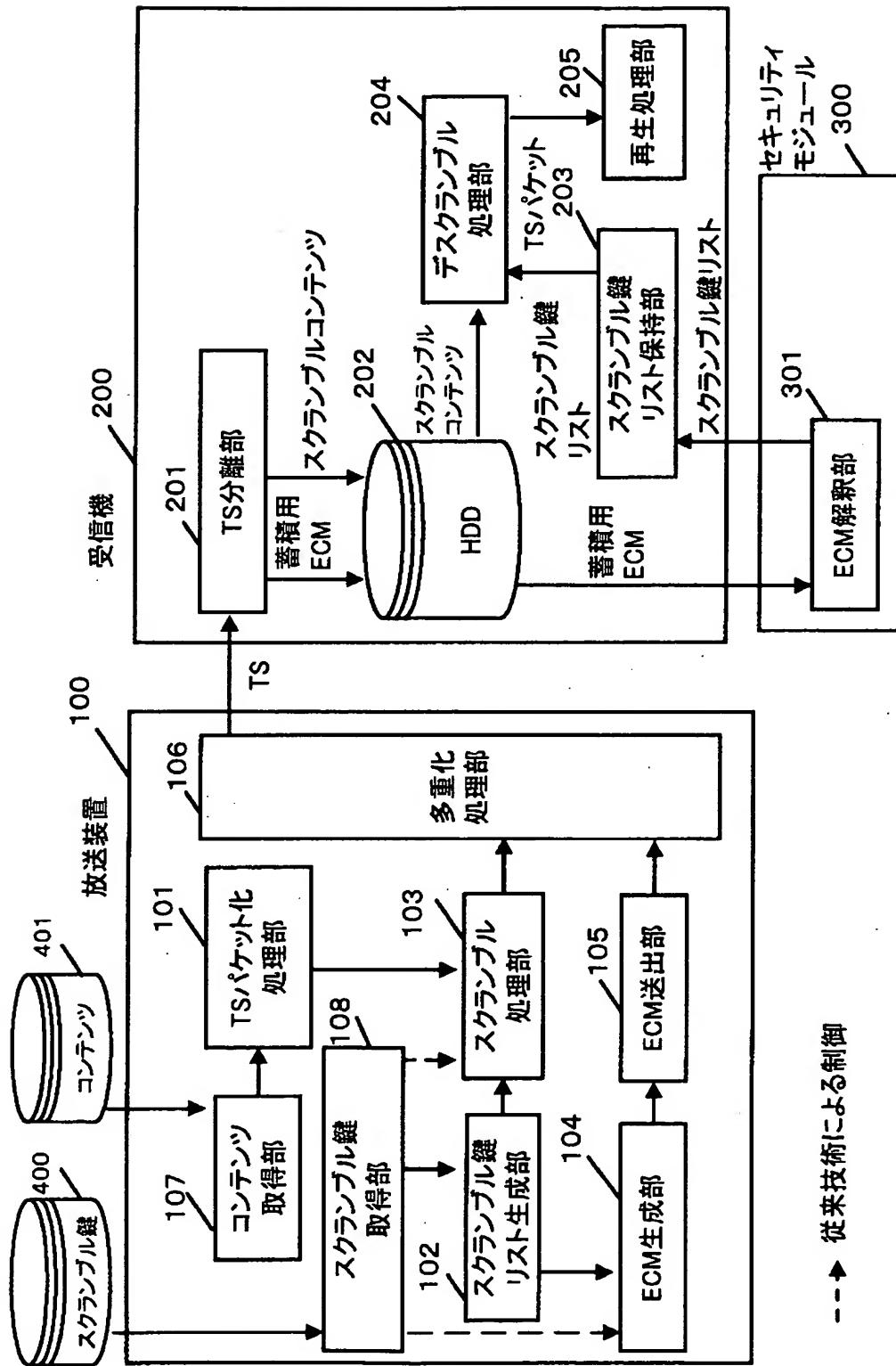
【符号の説明】

- 100 放送装置
- 101 TSパケット化処理部
- 102 スクランブル鍵リスト生成部
- 103 スクランブル処理部
- 104 ECM生成部
- 105 ECM送出部
- 106 多重化処理部
- 107 コンテンツ取得部
- 108 スクランブル鍵取得部
- 110 TSパケットカウンタ部
- 111, 122, 203 スクランブル鍵リスト保持部
- 112, 123 スクランブル部
- 113, 124, 212, 223 スクランブル鍵リスト解釈部
- 120, 221 スクランブル鍵識別子算出部
- 121 TSパケットヘッダ解釈部
- 200 受信機
- 201 TS分離部
- 202 HDD
- 204 デスクランブル処理部
- 205 再生処理部
- 210, 220 TSパケット抽出部
- 211, 222 デスクランブル部
- 300 セキュリティモジュール
- 301 ECM解釈部
- 400 スクランブル鍵
- 401 コンテンツ

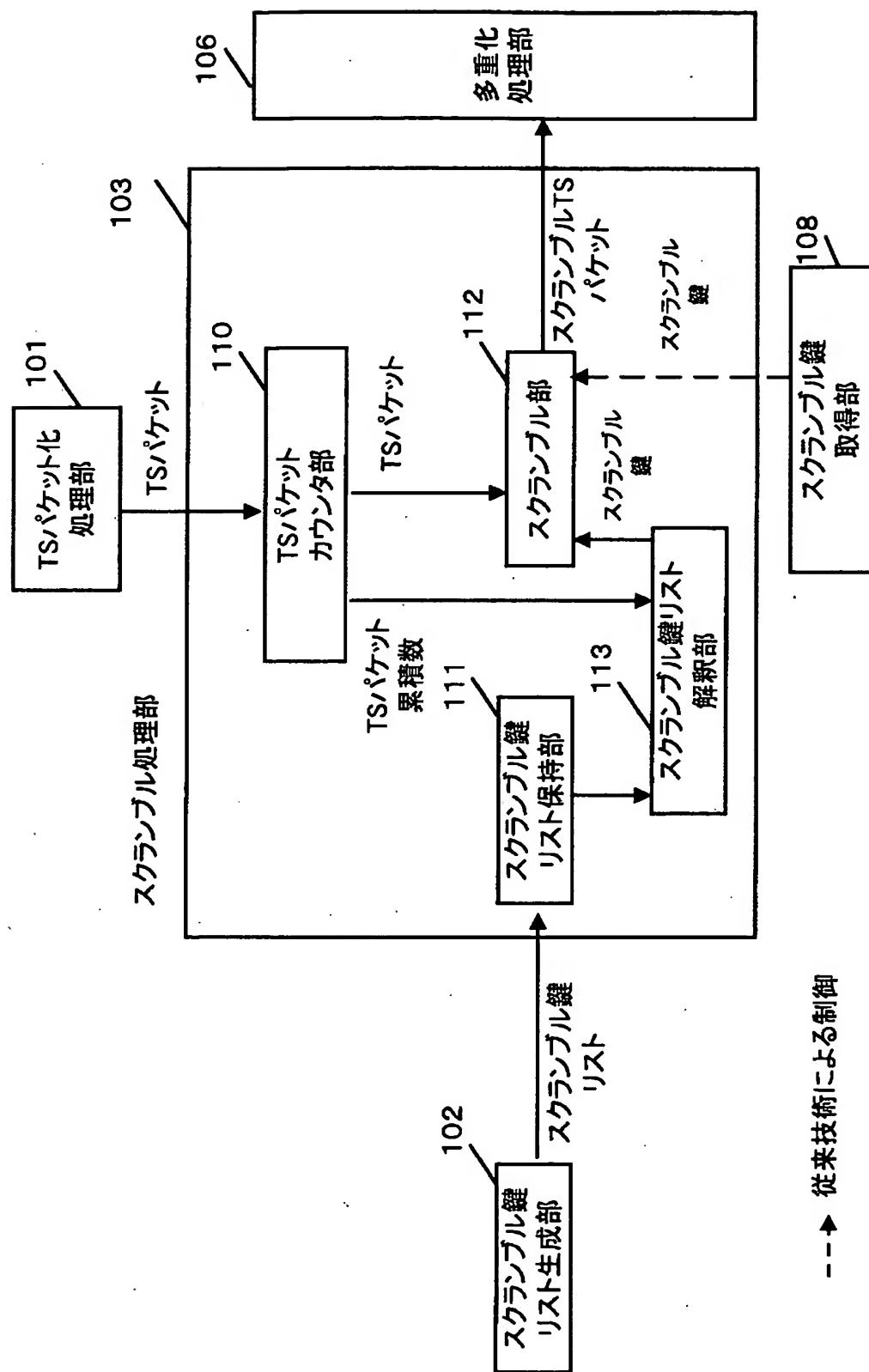
【書類名】

図面

【図1】



【図2】



【図3】

204

デスクランブル処理部



202



210

TS/パケット抽出部

スクランブル
TS/パケット

211

デスクランブル部

スクランブル鍵

212

スクランブル鍵リスト
解析部

TS/パケット

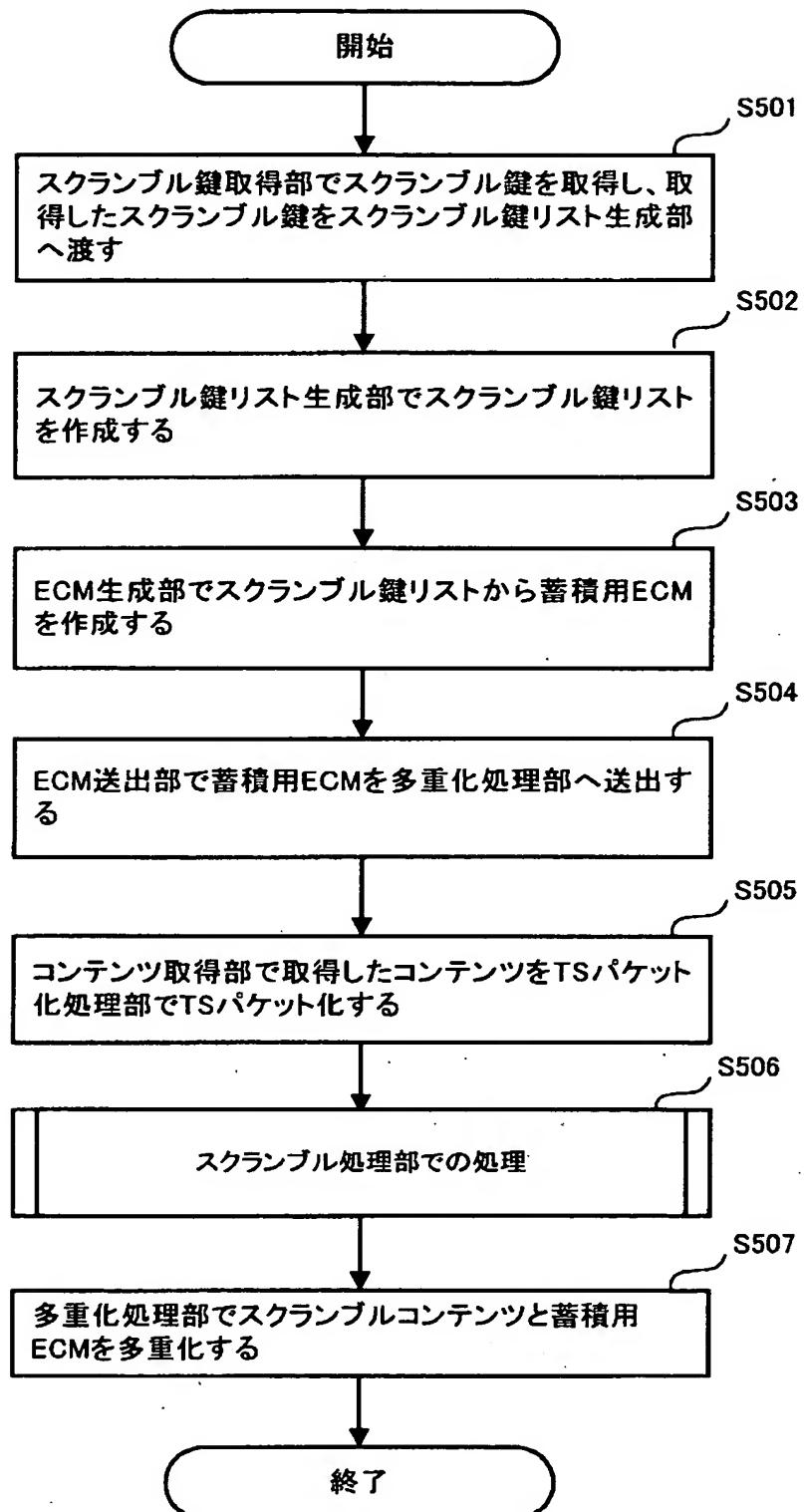
スクランブル鍵リスト
リスト保持部

205

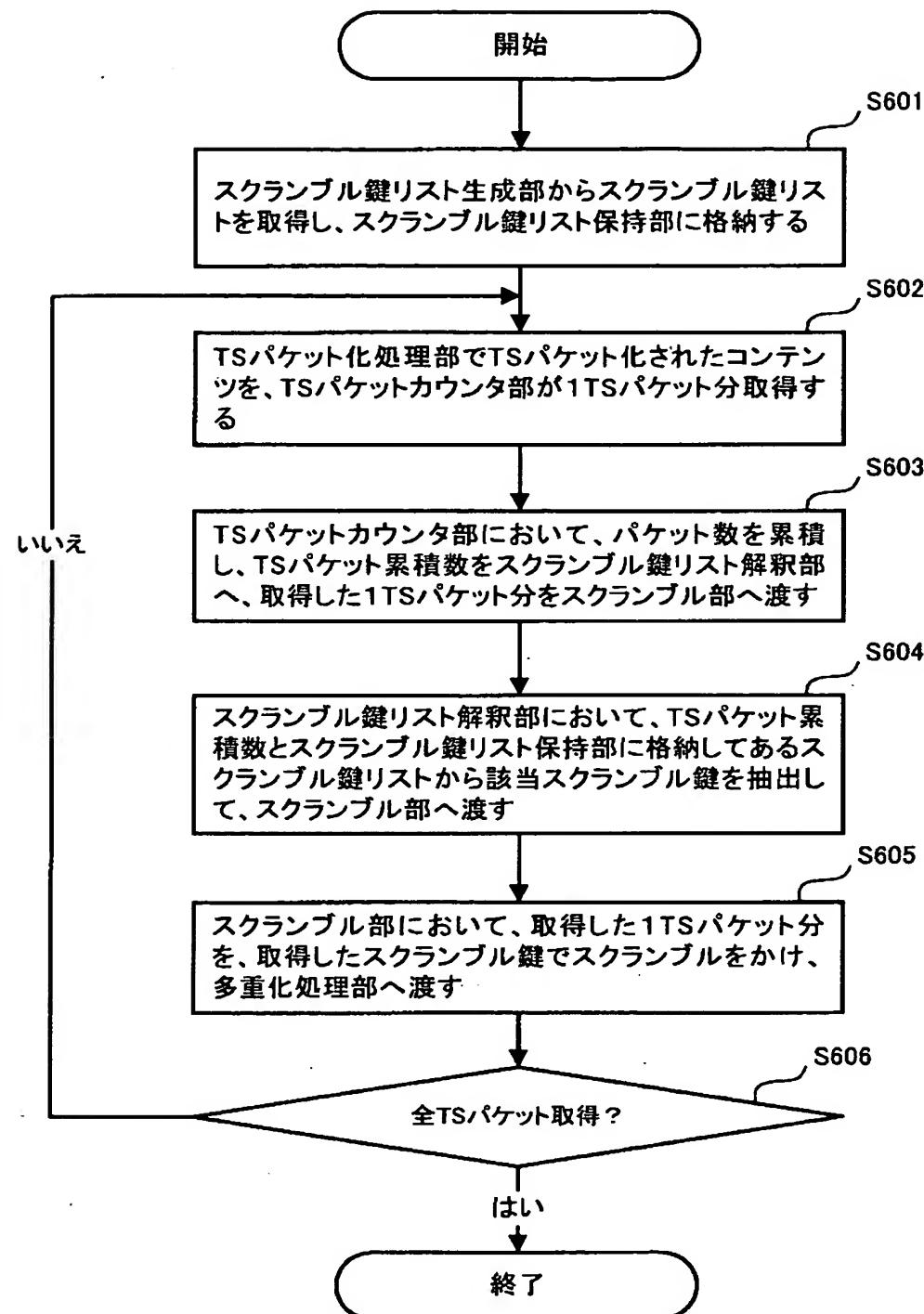
再生処理部

スクランブル鍵
リスト保持部

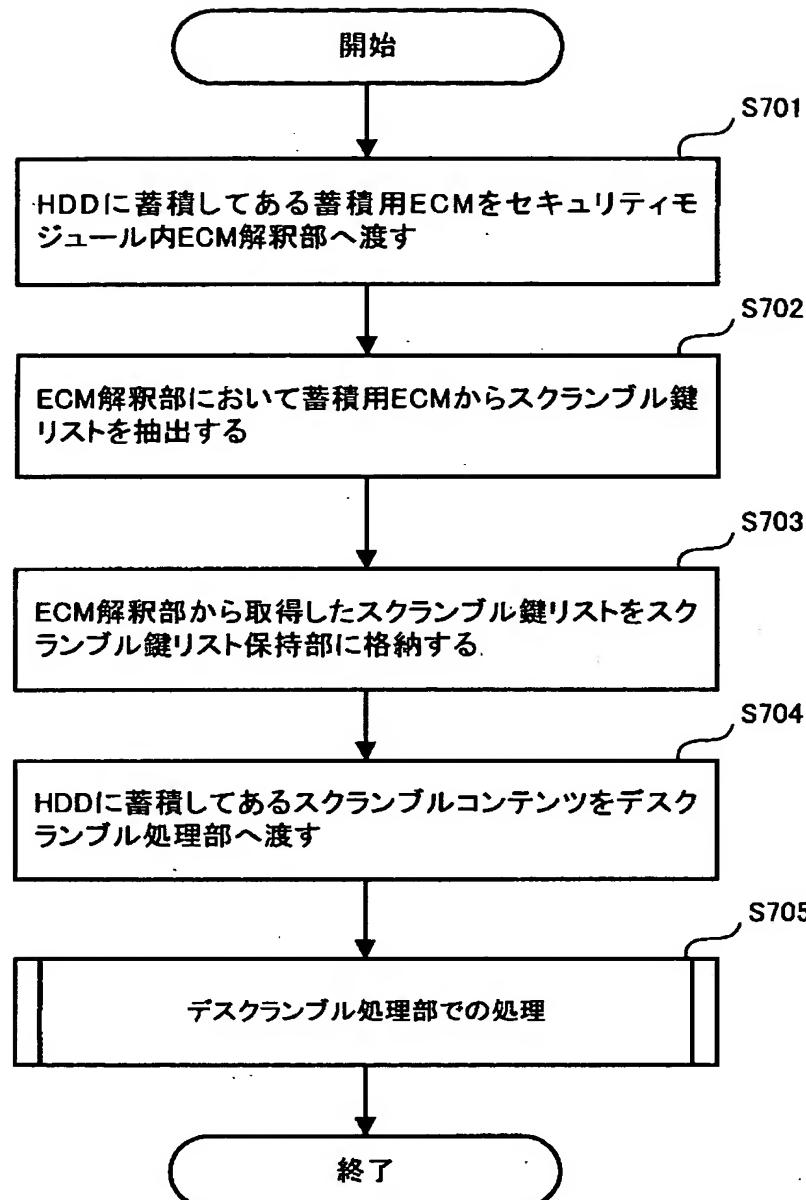
【図4】



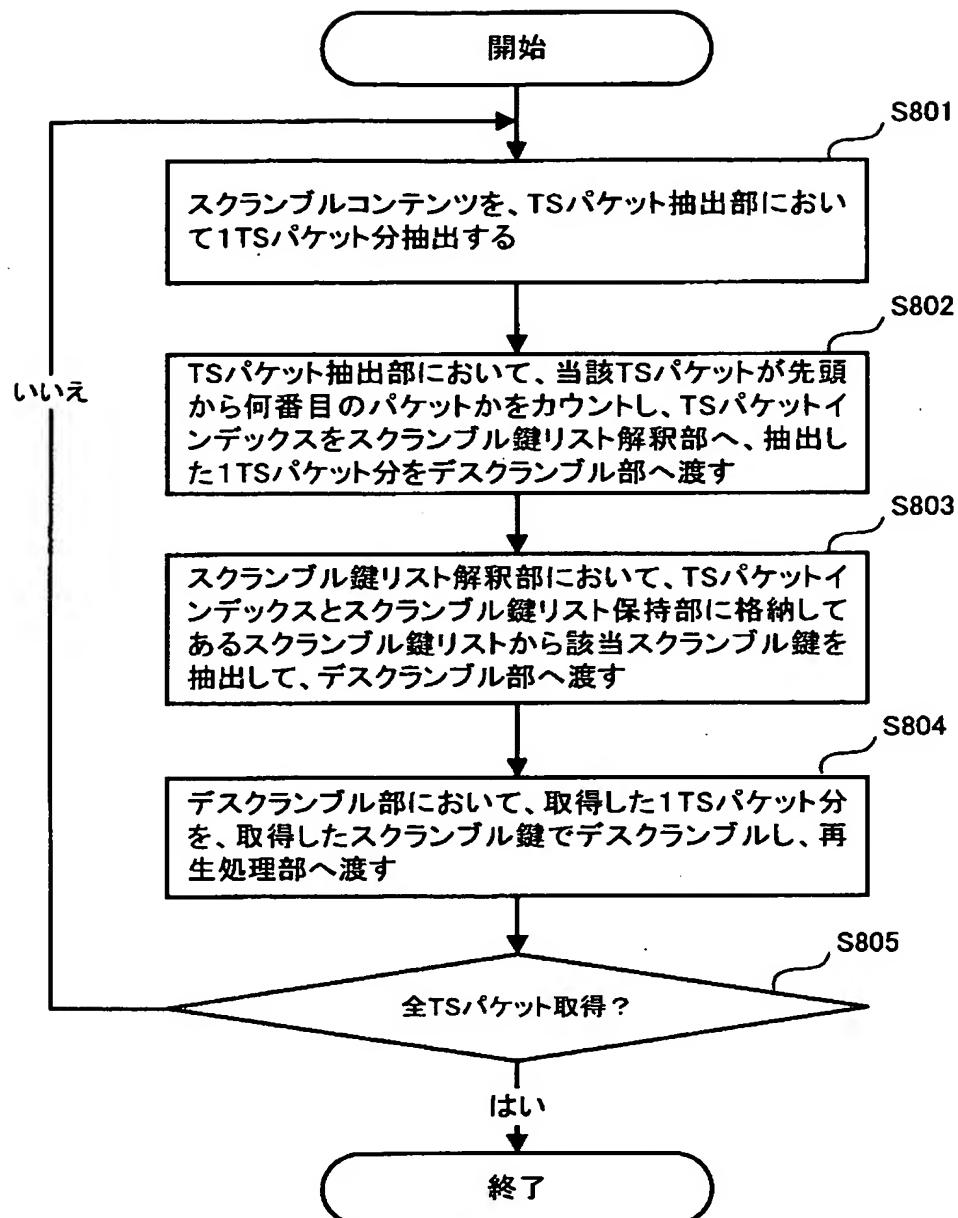
【図5】



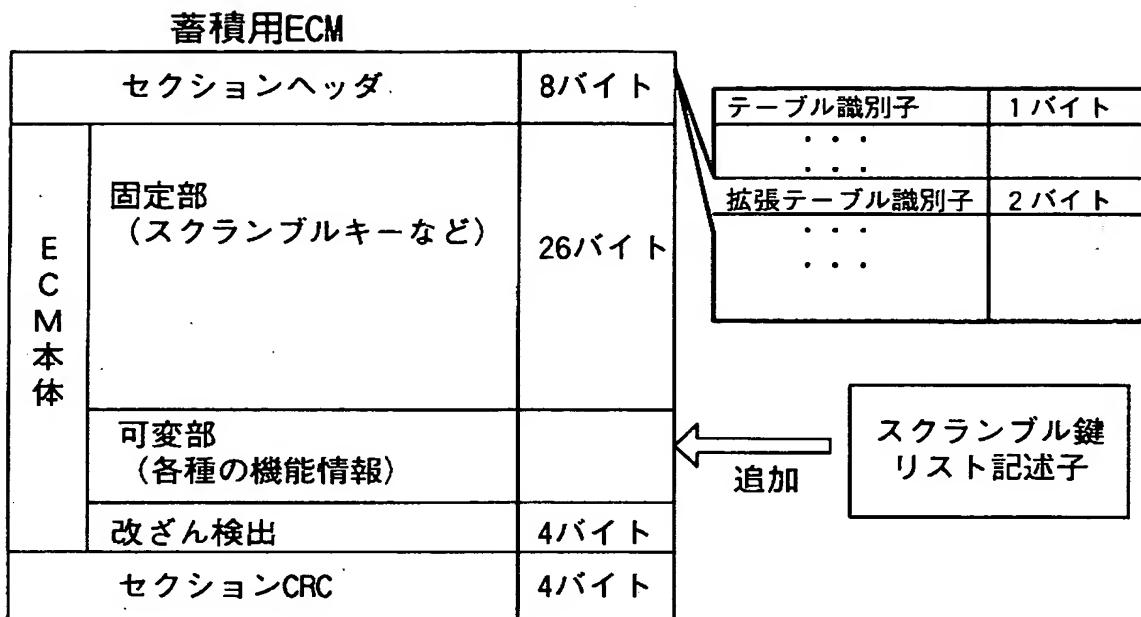
【図6】



【図7】



【図8】



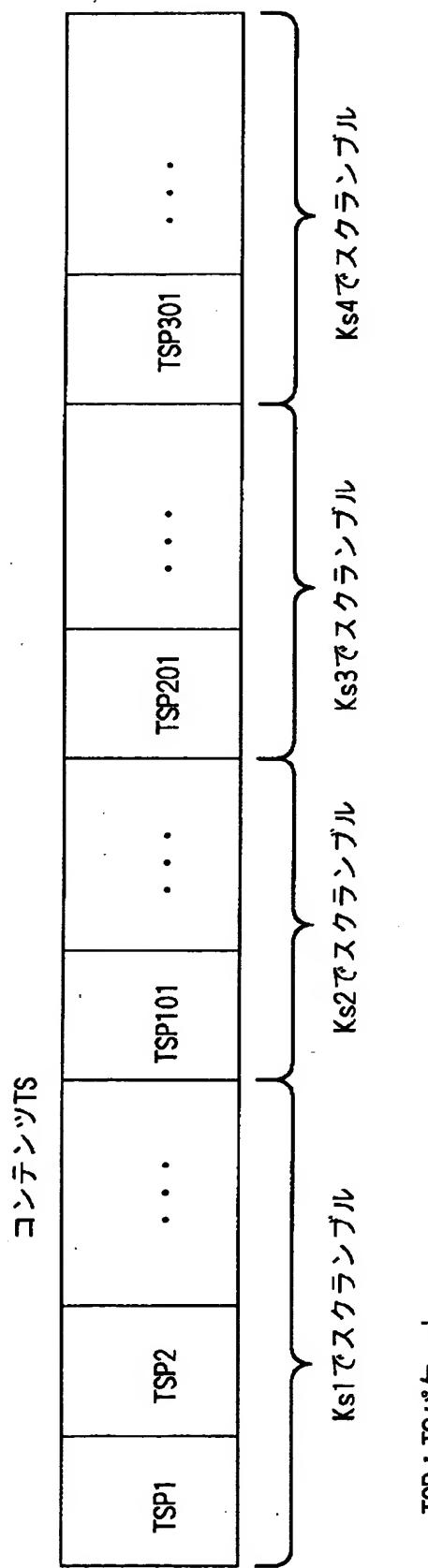
【図9】

スクランブル鍵リスト記述子のデータ構造

<pre>CA_Ks_List_descriptor() { descriptor_tag descriptor_length for(i=0;i<N;i++) { Ks_id TS_packet_number Ks } }</pre>	1バイト 1バイト 1バイト 2バイト 8バイト
---	--------------------------------------

Ks_id : スクランブル鍵識別子 (スクランブル鍵の識別をする)
 TS_packet_number : 当該KsでスクランブルしているTSパケット数
 Ks : スクランブル鍵

【図10】

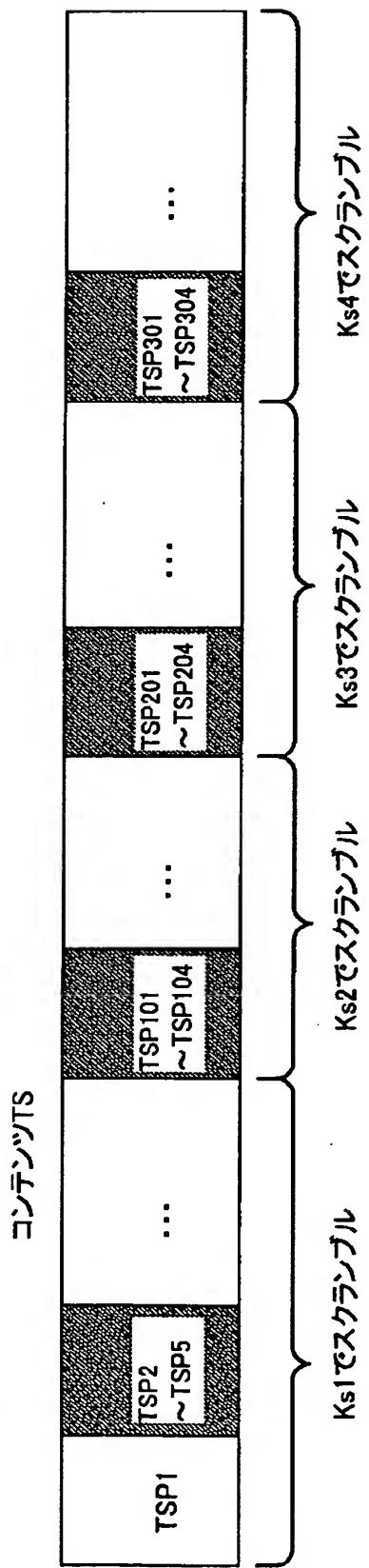


【図11】

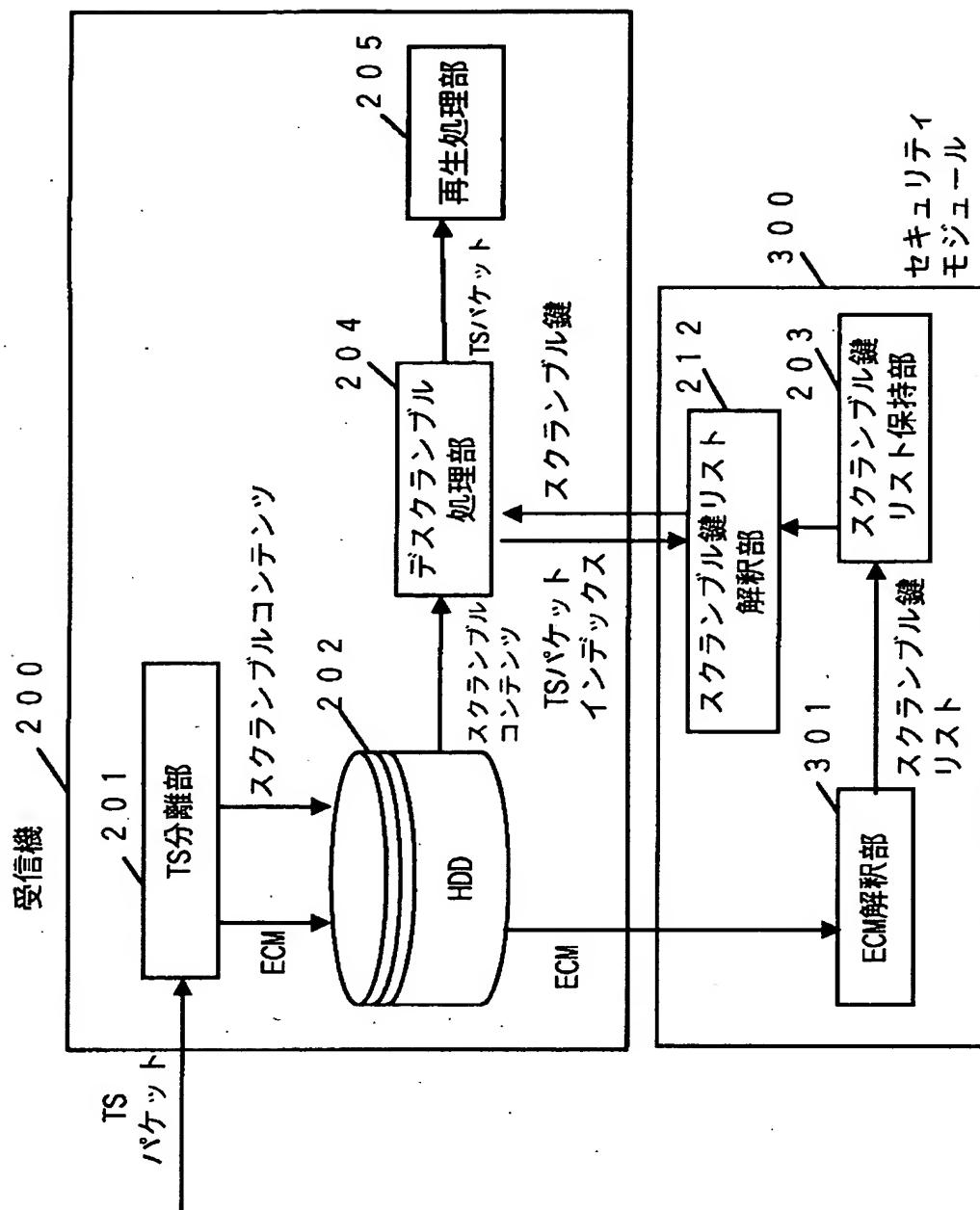
スクランブル鍵リスト

Ks_id	1
TS_packet_number	100
Ks	Ks1
Ks_id	2
TS_packet_number	100
Ks	Ks2
Ks_id	3
TS_packet_number	100
Ks	Ks3
Ks_id	4
TS_packet_number	100
Ks	Ks4

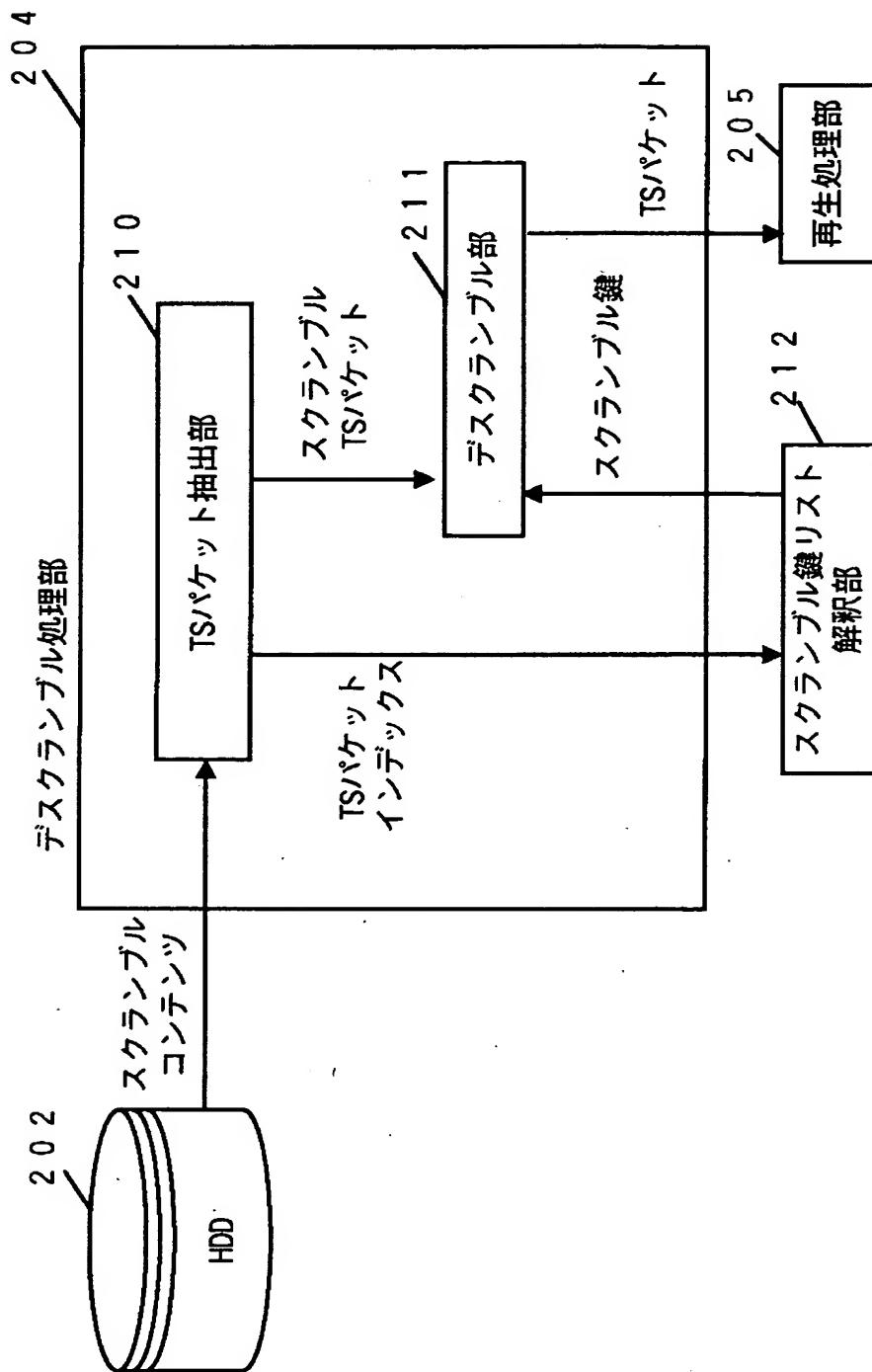
【図12】



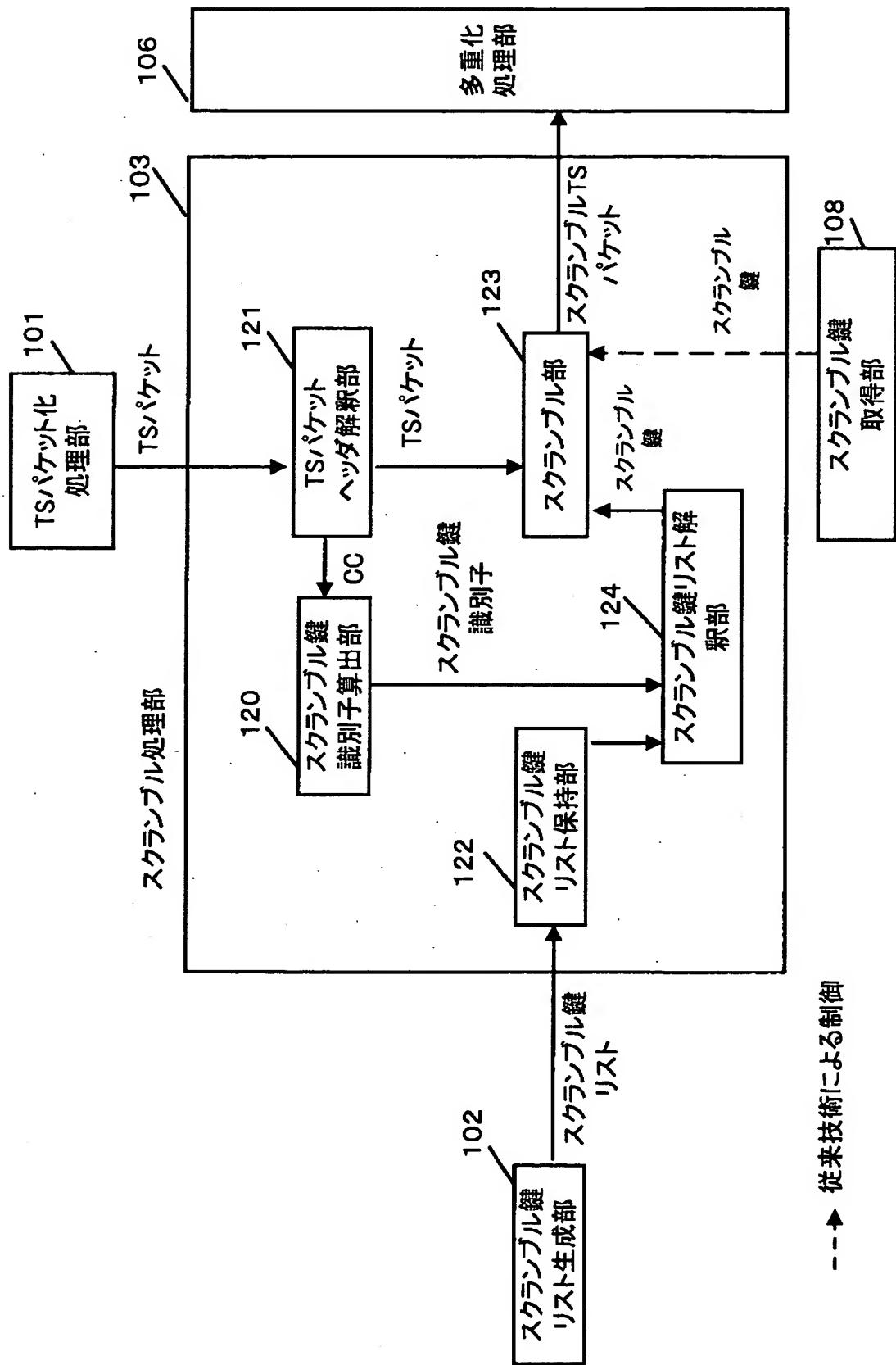
【図13】



【図14】



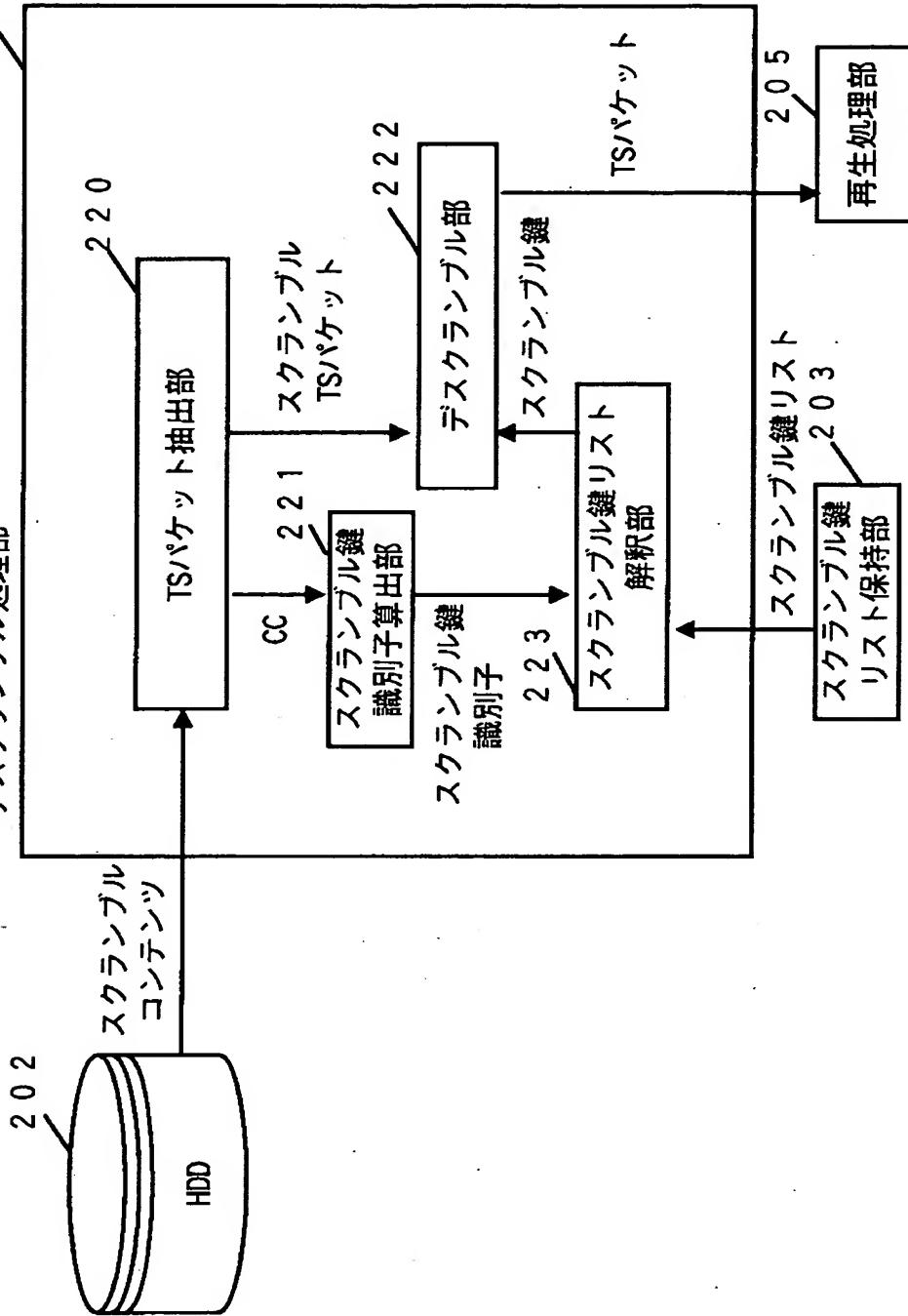
【図15】



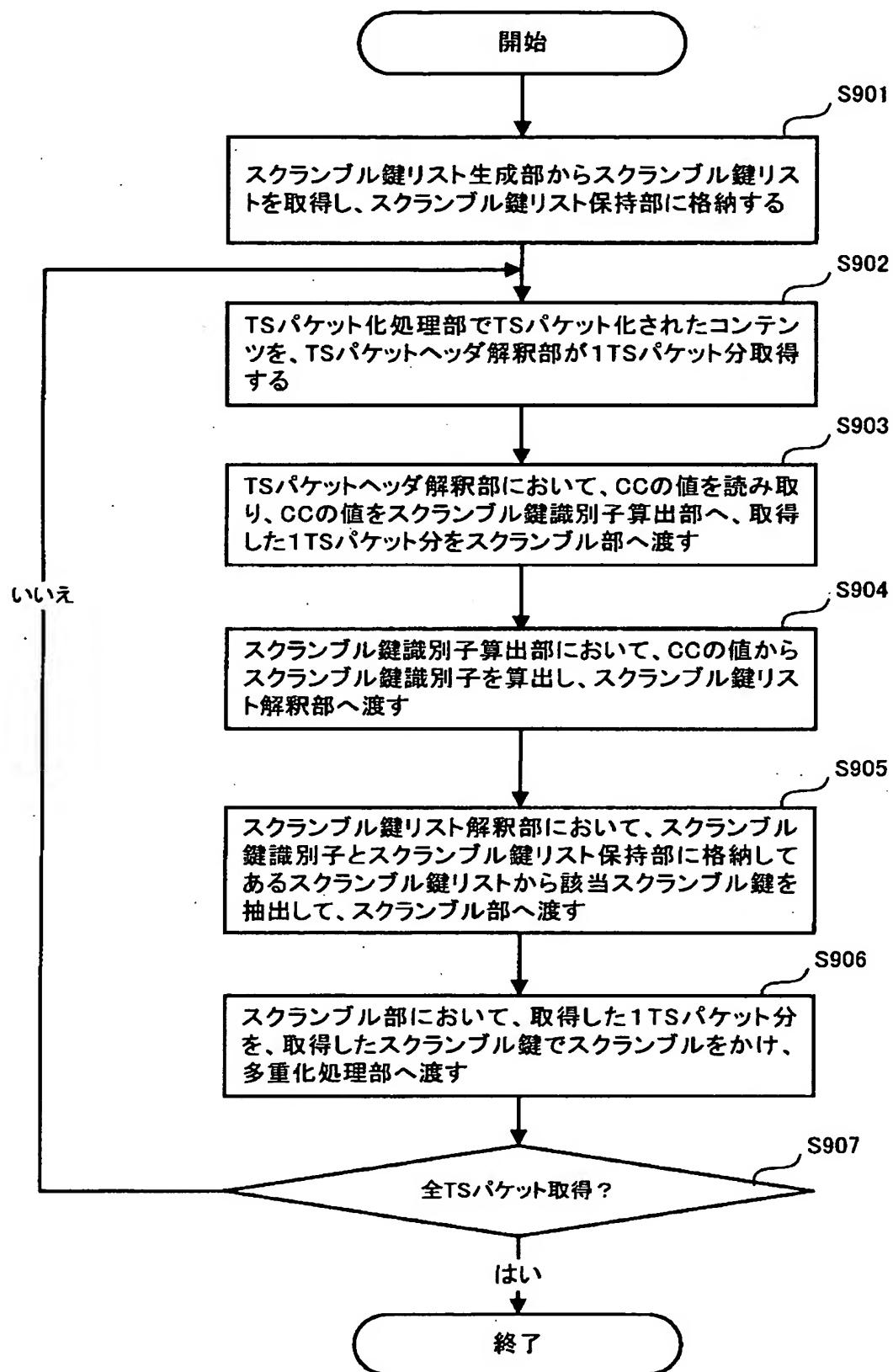
【図16】

204

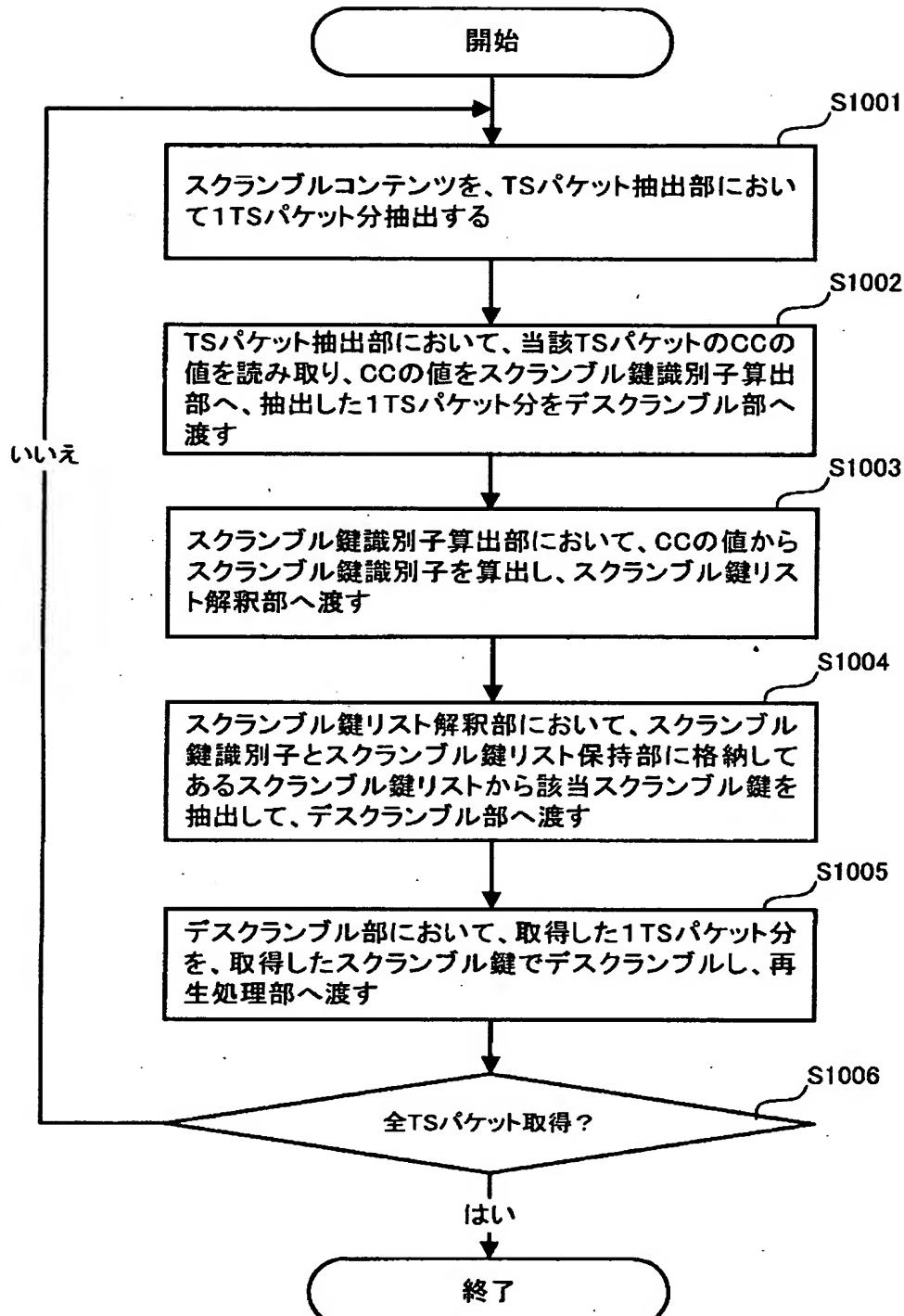
デスクランブル処理部



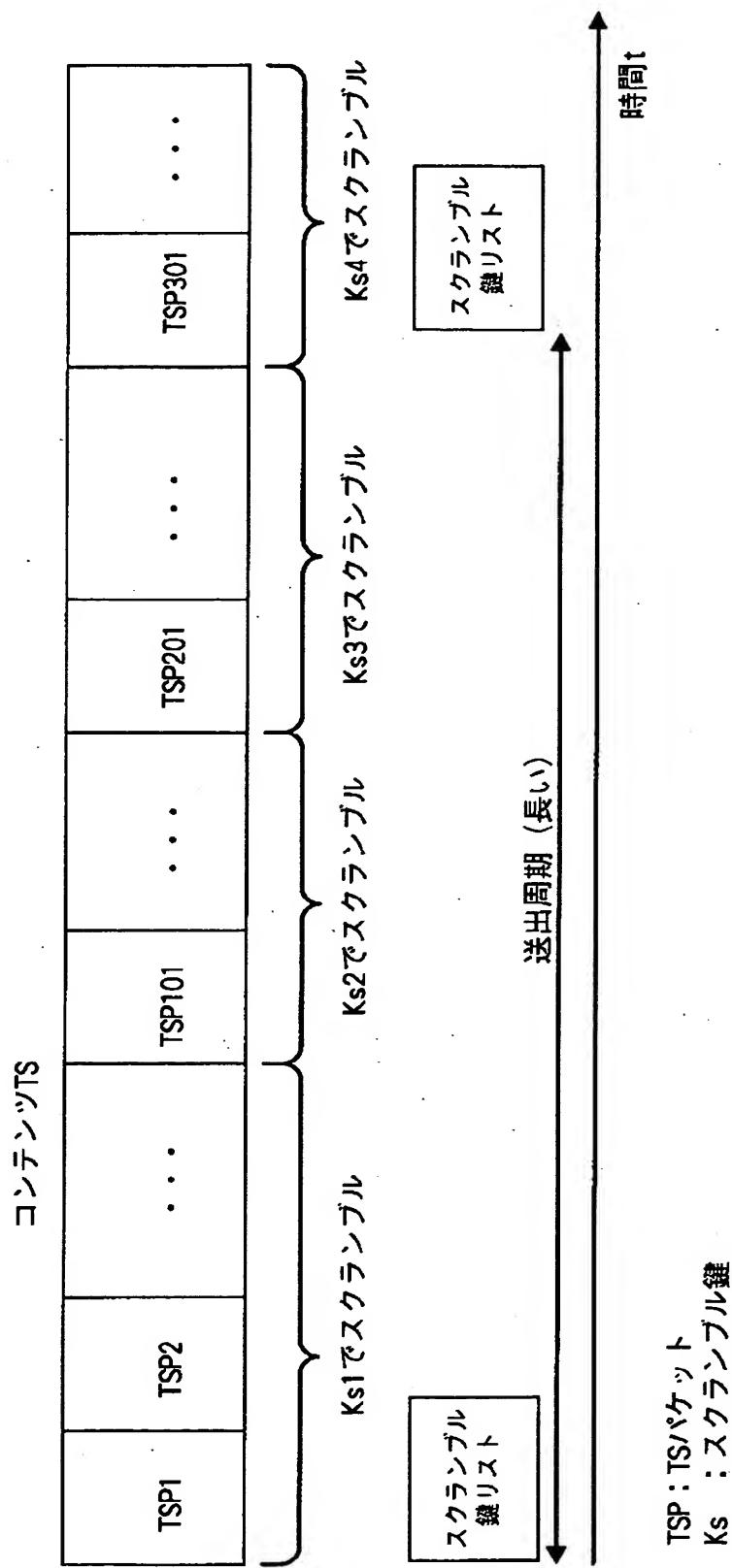
【図17】



【図18】



【図19】

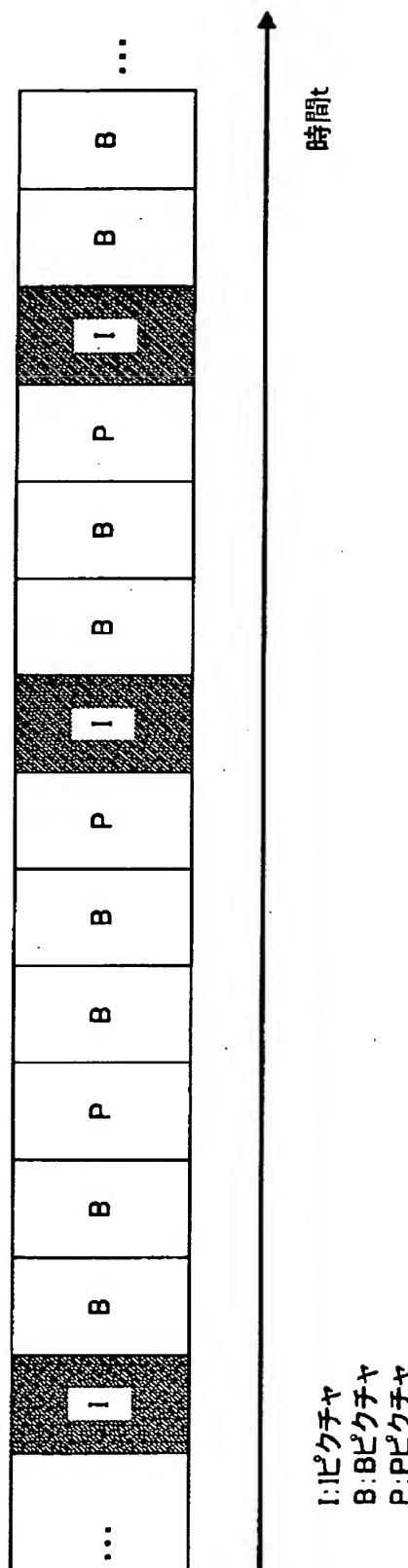


【図20】

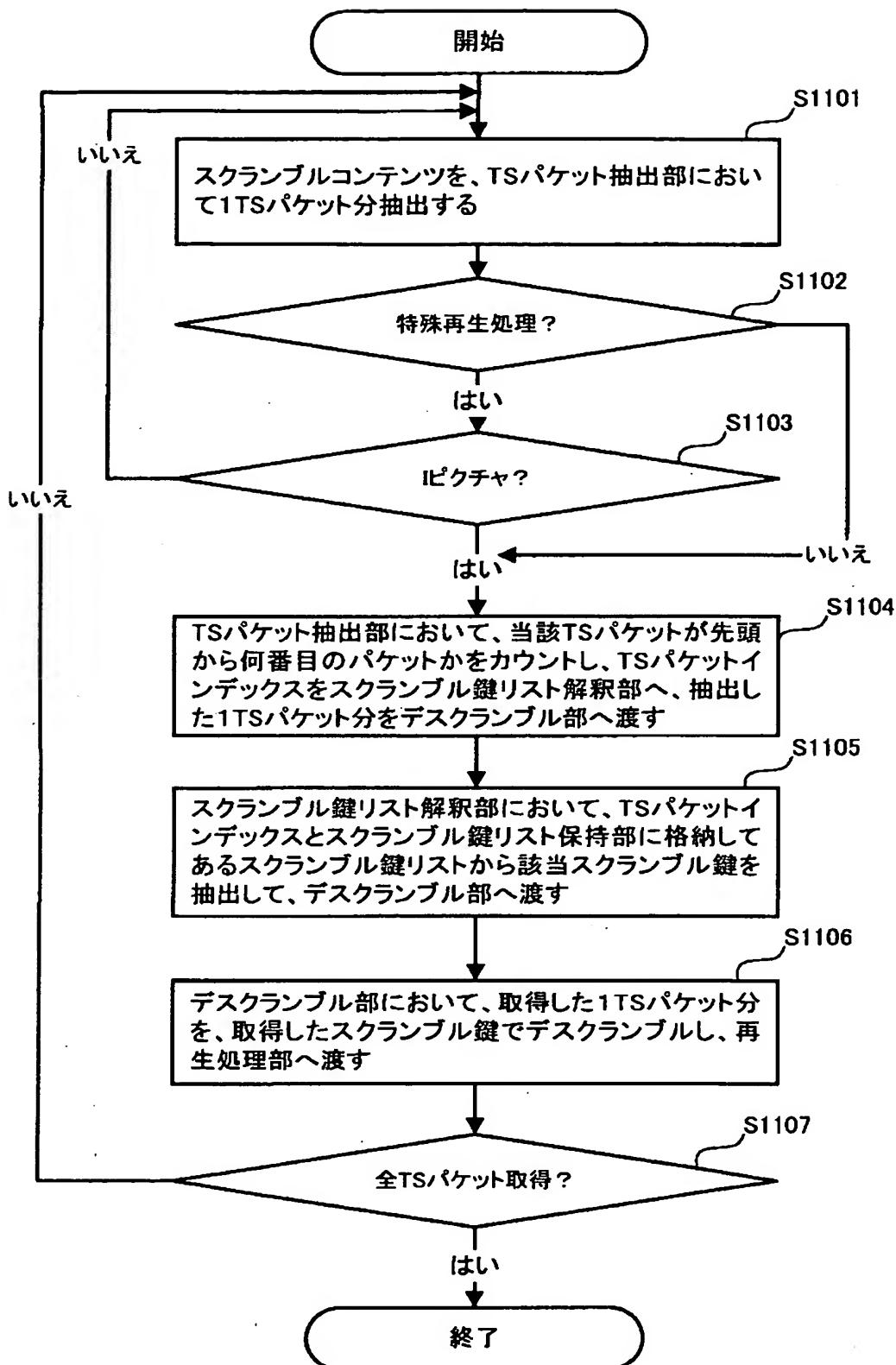
スクランブル鍵リスト

Ks_id	0
Ks	Ks1
Ks_id	1
Ks	Ks2
Ks_id	2
Ks	Ks3
Ks_id	3
Ks	Ks4
Ks_id	4
Ks	Ks5
Ks_id	5
Ks	Ks6
Ks_id	6
Ks	Ks7
Ks_id	7
Ks	Ks8
Ks_id	8
Ks	Ks9
Ks_id	9
Ks	Ks10
Ks_id	10
Ks	Ks11
Ks_id	11
Ks	Ks12
Ks_id	12
Ks	Ks13
Ks_id	13
Ks	Ks14
Ks_id	14
Ks	Ks15
Ks_id	15
Ks	Ks16

【図21】



【図22】



【書類名】 要約書

【要約】

【課題】 スクランブルコンテンツを蓄積し、蓄積後の特殊再生機能を、ユーザの満足できる性能で実現する。

【解決手段】 放送装置は、スクランブル鍵のリストを作成するスクランブル鍵リスト生成手段と、前記スクランブル鍵リストから蓄積用ECMを作成するECM生成手段と、前記蓄積用ECMを送出するECM送出手段と、TSパケット単位でスクランブルをかけるスクランブル処理手段を備え、受信機は、受信した蓄積用ECMからスクランブル鍵リストを抽出するECM解釈手段と、スクランブル鍵リストから該当TSパケットのスクランブル鍵を抽出するスクランブル鍵リスト解釈手段と、TSパケット単位でデスクランブルするデスクランブル処理手段とを備える。

【選択図】 図1

出願人履歴情報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住 所 大阪府門真市大字門真1006番地
氏 名 松下電器産業株式会社